International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 2, Mar 2014, 131-140

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

OPTIMIZING THE EFFICIENCY OF WATCHDOG IDS IN MANETs USING SELFISHNESS INFORMATION AND BAYESIAN FILTERING

VARSHA HIMTHANI[1], PRASHANT HEMRAJANI[2] & SACHIN SHARMA[3]

[1]Department of Computer Science and Engineering, MAIET, Jaipur, Rajasthan, India

[2]Department of Computer Science and Engineering, Poornima University, Jaipur, Rajasthan, India

[3]Department of Computer Science and Engineering, RIET, Jaipur, Rajasthan, India

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are a new paradigm for wireless communication for mobile hosts. These Networks do not need the costly base stations as in wired networks or mobile switching centers in cellular wireless mobile networks. In such a network, each node acts as an end system as well as a relay node (or router). Routing protocol for MANETs are designed based on the assumption that all the participating nodes are fully cooperative. However, nodes may become selfish due to low battery life remaining. This selfishness is a characteristic property of any node which is provided by the device manufacturer so as to maximize the node life before being fail due to exhausted battery. Depending upon the probability distribution of mean number of packets to be transferred by any node in the network, one can calculate the average life of a node before it attains selfish behavior. Also, there is always a scope of intruder attacking and harming the usual functioning of the Network, which may cause a node to perform maliciously thereby forwarding packets in unusual way to the unauthorized. The watchdog is a well-known sensor usually adopted for detecting black-holes in such networks, but typical watchdogs are characterized by a relatively high number of false positive and negative cases, which can affect the effectiveness and efficiency to deal with intrusions. This paper proposes a novel approach for detecting selfish node in mobile P2P networks by using Bayesian Filtering and an estimation of the mean time to get selfish for any node.

KEYWORDS: MANET, Selfishness

I. INTRODUCTION

Mobile Ad hoc NET works (MANETs), are distributed systems composed by wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary topologies [1]. These networks have origins in military missions and recovery operations but, in the recent years, a wide range of possible civil applications emerged, e. g., vehicular networks (VANETs), a form of Peer to Peer [2] mobile networks used for communication among vehicles and between vehicles and roadside equipment. The main characteristic of such networks is that they allow different kinds of devices to easily interconnect in areas with no pre-existing communication infrastructure; there exist several protocol specifications, such as AODV [3], that aim to find routing paths between pairs of devices.

These allow non-neighboring nodes to communicate by using intermediate nodes as relays. But the majority of these protocols assume a friendly, reliable and cooperative environment. Therefore, a single malicious node can easily prevent a mobile network from working and therefore the emerging need for research focused on the provision of practical proposals for securing them.

There have been numerous contributions to secure wireless networks, including key management, secure routing, Byzantine detection, and various protocol designs. Countering these types of threats is particularly important in military communications and networking, which are highly dynamic in nature and must not fail when adversaries succeed in compromising some of the nodes in the network. The problem of solution scheme for Byzantine detection is that it is receiver-based, that is, the receiver of the corrupted data detects the presence of an upstream adversary. However, this detection may come too late as the adversary is partially successful in disrupting the network (even if it is detected). It has wasted network bandwidth, while the source is still unaware of the need for retransmission. Watchdog and Pathrater [6] are protocols in which upstream nodes police their downstream neighbors using promiscuous monitoring. Promiscuous monitoring means that if a node v is within range of a node v_0, it can overhear communication to and from v_0 even if those communications do not directly involve v. This scheme successfully detects adversaries and removes misbehaving nodes from the network by dynamically adjusting the routing paths. However, the protocol requires a significant overhead owing to increased control traffic and numerous cryptographic messages.

The problem of all the current ad hoc routing protocols is that they trust all nodes and assume that they behave properly; therefore they are vulnerable to attacks launched by misbehaving nodes. The resource limitation of nodes used in MANET, along with the multi-hop nature of this network may cause a new phenomenon which does not exist in traditional networks. To save its resources, nodes may behave selfishly and uses the services of other nodes without correctly participate in system. Watchdog [11] method is a reputation based method used for the detection of selfish nodes and Black holes in MANETS. A watchdog continuously listening neighboring devices for verifying that they, when they are not the final expected recipients, forward packets/messages toward the final destinations. Indeed in MANETs every node is able to analyze the packet headers and learn whether neighboring nodes are the actual receivers or, conversely, they should forward it to another node on the path to the destination. Devices that do not forward packets for which they are not recipient are considered as misbehaving. Malicious nodes' detections of current-day watchdogs are affected by several errors due to nodes' mobility and signal noises. This work aims at providing more accurate measures of detection of maliciousness/selfishness by integrating Bayesian watchdogs with Probability distribution of failure times of nodes. Bayesian filters can partly fade the problems by using historical information obtained by the watchdog in the previous time. The technique proposed is independent of the underlying routing protocols and, hence, is widely applicable in several different scenarios of P2P mobile networks. Standard Watchdog Implementation, along with Bayesian Filtering [12], provides a much more improved estimation for detection of selfish nodes in MANETs. This Bayesian Watchdog can be further improved by inculcating the mean time for nodes to get selfish so that more accurate estimation can be obtained for proper routing. The objective of the research is to improve the estimation of probability of packet delivery to the destination, as computed on every hop node on the path, using Bayesian Filtering and Probability Distribution. Probability of any node being selfish or not is computed using a set of observations witnessed by nodes on the path under consideration.

II. LITERATURE SURVEY

Wireless communication networks, mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs) in particular, have undergone tremendous technological advances over the last few years. With this development comes the risk of newer threats and challenges, along with the responsibility of ensuring the safety, security, and integrity of information communication over these networks. MANETs, due to the individualized nature of the member nodes, are

particularly vulnerable to selfish behavior. Because each node labors under a energy constraint, there is incentive for a node to be programmed to selfishly guard its resource, leading it to behave in a manner that is harmful to the network as a whole. Reputation is the opinion of one entity about another. In an absolute context, it is the trustworthiness of an entity. Trust, on the other hand, is the expectation of one entity about the actions of another. For over three decades, formal studies have been done on how reputation and trust can affect decision making abilities in uncertain conditions. Only recently has trust and reputation been adapted to wireless communication networks. Trust is a multidimensional entity which, if effectively modeled, can resolve many problems in wireless communication networks.

A. Misbehavior of Nodes

The non-cooperative behavior of a node in a MANET as identified in, is mainly caused by two types of misbehavior: selfish behavior e.g., nodes that want to save power, CPU cycles, and memory, and malicious behavior which are not primarily concerned with power or any other savings but interested in attacking and damaging the network. Karl of and Wagner [13] have identified various types of security threats in a WSN. There exist three other types of routing misbehavior: Blackhole, Grayhole, and Wormhole [15].

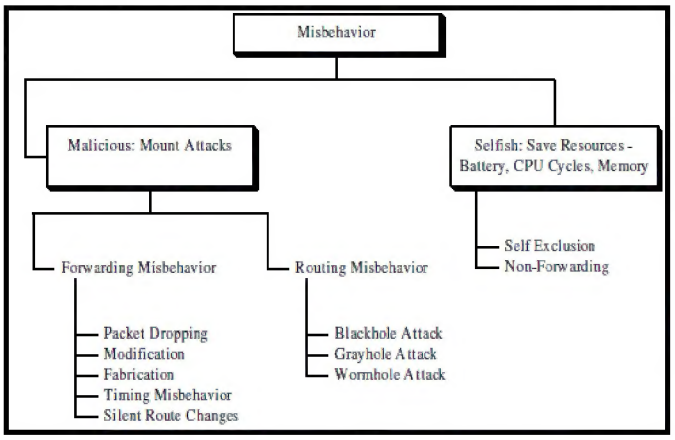

Figure 1: Node Misbehavior in MANETs

The selfish behavior of a node can be generally classified as either self-exclusion or non-forwarding. The self exclusion misbehavior is one in which a selfish node does not participate when a route discovery protocol is executed. This ensures that the node is excluded from the routing list of other nodes. This benefits a selfish node by helping it save its power, as it is not required to forward packets for other nodes. Researchers have been steadily making efforts to successfully model WSNs and MANETs as reputation and trust-based systems [15]. Adapting reputation and trust-based systems to WSNs presents greater challenges than MANETs and Peer-to-Peer (P2P) [16] systems due to their energy constraints. There are various systems for WSNs, MANETs and P2P networks.

B. Effects of Node Misbehavior

In wireless networks without appropriate countermeasures, the effects of misbehavior have been shown by several simulations is to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their specific strategies, network throughput can be severely degraded, packet loss increased, and denial-of-service experienced by honest nodes in the network. In a theoretical analysis of how much cooperation can help by increasing the probability of a successful forwarding of packets, it has been found that increased cooperation more than proportionately increases the performance for small networks with fairly short routes.

Also, prevention measures, such as encryption and authentication can be used in MANETs to reduce the success of intrusion attempts, but cannot completely eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which carry the private keys. No matter what types of intrusion prevention measures are deployed in the network, there are always some weak links that an adversary can exploit to break in. Intrusion detection presents a second wall of defense and it is a necessity in any high-survivability network.

C. Watchdog

The watchdog is a well known Intrusion Detection System (IDS) for MANETS. It allows detecting misbehaving nodes. The watchdog method detects misbehaving nodes. The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet.

III. BAYESIAN WATCHDOG [22]

The standard watchdog simply overhears the packets transmitted and received by its neighbors, counting the packets that should be retransmitted, and computing a trust level for every neighbor as the ratio of "packets retransmitted" to "packets that should have been retransmitted". If a node retransmits all the packets that it should have retransmitted, it has a trust level of 1. If a node has a trust level lower than the configured tolerance threshold, that node is marked as malicious or selfish. The role of the Bayesian filter in the watchdog is to probabilistically estimate a system's state from noisy observations. As a result of their work, Hortelano et al. [8] found that, compared to the standard one, the Bayesian watchdog reaches a 20% accuracy gain, and it presents a faster detection on 95% of times. So, this Bayesian watchdog is an excellent brick to build a MANET-wide system to detect black hole nodes even earlier and more accurately, through collaboration between nodes running this watchdog version.

Mathematically, the Bays theorem is as follows:

P(h/e)=[P(e/h)*P(h)] / [P(e)]

P(h) is called the prior probability of hypothesis and P(e) is called the prior probability of evidence.

P(h/e) is the probability of h given e, and P(e/h) is the probability of e given h.

Hence when all the values are supplied (i.e. prior probabilities) the Bays theorem computes the posterior probability. Using the Bayesian Approach similar to that use in e mail filtering, the Bayesian Filter detects the probability of a node being cooperative or malicious.

The Bayesian watchdog presented here makes use of the Beta Probability Distribution as given below:

$$B(\alpha,\beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}dx$$

The corresponding Beta Probability Density Function is

$$Pr(x|\alpha,\beta) = x^{\alpha}(1-x)^{\beta} / B(\alpha,\beta)$$

Here, x denotes the probability that the node j, which is under surveillance of node i, is cooperative. The watchdog

of device i is in charge of listening the packets' traffic in its neighborhood and verifying whether the fraction of packets that are not correctly forwarded by every neighboring device j. If a given j forwards less than a given fraction of packets than it should, the watchdog considers j as misbehaving. Device i does not know a priori such a fraction for each neighboring node j and, therefore, it defines a random variable $\theta i(j)$ to estimate it for j. In fact, $\theta i(j)$ is the viewpoint of device i for what concerns device j. It is worthy highlighting that taking only the last observation is not sufficiently reliable since this could be effected by noise. So the old observations should be considered. Therefore, the watchdog makes use of Bayesian filtering. Variable $\theta i(j)$ complies with the Beta distribution with parameters ($\alpha^{(i,j)}$, $\beta^{(i,j)}$). These parameters are continuously updated with new incoming observations of the fraction of non-forwarded packets. Node i makes periodical observations each t seconds (with t constant) of the behavior of node j. Let s be the fraction of packets observed by i that are not forwarded by node j in this observation period. Parameters $\alpha^{(i,j)}$ and $\beta^{(i,j)}$ are updated as follows:

$\alpha^{(i,j)} = u*\alpha^{(i,j)} + s$; estimate of maliciousness

$\beta^{(i,j)} = u*\beta^{(i,j)} + (1-s)$; estimate of cooperativeness

Values $\alpha^{(i,j)}$ and $\beta^{(i,j)}$ are initially set to 1.

Here, α and β denote the estimated values and if $\beta - \alpha \geq \tau$ (threshold), one can state with certain probability that the node is cooperative or else, its behavior is unpredictable.

The variable u is a fading mechanism for past experiences. This fading mechanism allows for redemption of a neighbor if its behavior changes to a correct one along the time. This fading mechanism will be useful if there are false positives due to the environmental noise. Greater values for u correspond to consider the old observations more significantly. The above formulation is based on the assumption of false negative and false positive probabilities about the behavior of the node. The parameter u can be derived from stochastic modeling of the behavior of MANET.

A. Augmenting Bayesian Watchdog with Selfishness Information

Consider a MANET consisting of N nodes. let λ be the mean number of packets transmitted per unit time by any node and this packet transmission follows Poisson Distribution. Let t be the time between consecutive observations for updating the values of the parameters α and β. The mean number of packets transmitted in time t is $\lambda*t$.

The probability of k transmissions in time t is given by;

$P(n = k) = (\lambda*t)^k e^{-(\lambda*t)} / k!$ [equation 3.1]

Let P_{trans} be the power consumption in a packet transfer abd let P_0 be the total available power in the node initially as provided by the battery. let $P_{selfish}$ be the power in the battery before the node gets selfish, then the expected number of cooperative transmissions before the node gets selfish is:

$T = P_0 - P_{selfish} / P_{trans}$ [equation 3.2]

The value T is a constant for a particular type of network. The value u must depend on E and T for a close approximation on the decision about the behavior of node. Thus, u must be chosen as a suitable function of E_m and T. The quantity $T-E_m$ denotes the mean number of packets that can be transmitted before the node becomes selfish. The parameter α is a measure of selfishness, and the parameter β is a measure of cooperativeness. The parameter β must be correlated to k must be set to zero after k^{th} observation, where

$k = T — E_m / \lambda t$

B. Packet Transmission Probability with Varying Mean Rates

Consider a MANET with n nodes, each transmitting packets with mean rate λ per unit time. The packet transmission probability of k packets in a unit time can be best modeled through Poisson Probability Distribution and is given by equation 3.1, repeated here for ready reference.

$P(n = k) = (\lambda * t)^k e^{-(\lambda * t)} / k!$

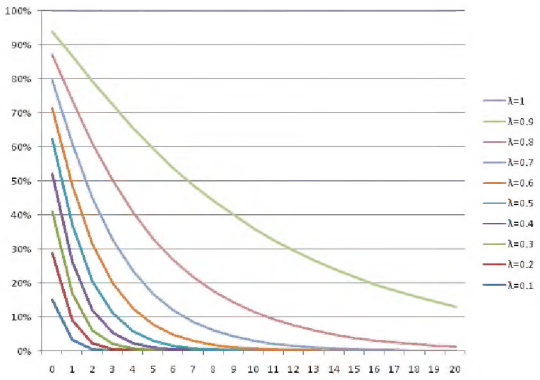

Figure 2: Various Probabilities Accordance to Various Transmission Rates as per Poisson Probability Distribution

C. Mean Time to Attain Selfish Behavior with Various Transmission Sion Rates

The expected number of cooperative transmissions before a node attains selfish behavior is given by the equation 3.2 repeated here for ready reference

$T = P_0 — P_{selfish} / P_{trans}$

Assuming the following values for the parameters:

Initial Battery Power: 10 Watt

Selfishness Criteria: 1 Watt (Before Attaining Selfishness)

Power Consumption in Single Packet Transmission: 0.1 Watt

Therefore, average number of packets forwarded before the node attains selfish behavior is 90. In accordance with various mean rates of packet transmission, the mean time to get selfish can be computed.

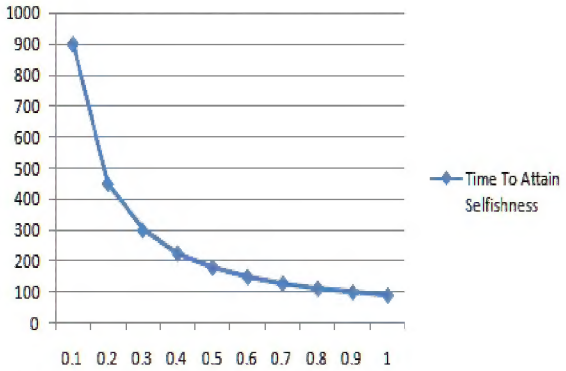

Figure 3: Time to Attain Selfish Behavior with Varying Rates of Packet Transmission

D. The Beta Probability Distribution for Detection of Selfish Nodes

Consider the following values of parameters for Beta Probability Density Function to decide whether the node under consideration is selfish or malicious.

Lower Bound Value: 0 (These are the values between which the probabilities are considered)

Upper Bound Value: 1

α: Initially set to one (updated uniformly as given in Chapter 3)

β: Initially set to one (updated uniformly as given in Chapter 3)

Table 1: Beta Probabilty Densitiy under Given Settings

Round	α	β	Probability
0	1	1	0.5
1	0.9	1.1	0.569077
2	0.8	1.2	0.636737
3	0.7	1.3	0.701625
4	0.6	1.4	0.762505
5	0.5	1.5	0.81831
6	0.4	1.6	0.868184
7	0.3	1.7	0.911513
8	0.2	1.8	0.947944
9	0.1	1.9	0.977385

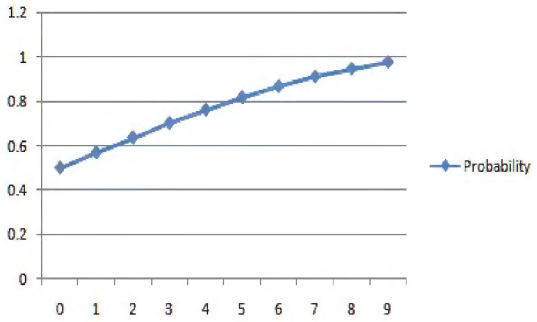

Figure 4: Probability Density Function as per Table 1

The given plot clearly indicates that more precise value of probability density is obtained as the values of the parameters get refined. This refinement comes as the cost of an additional estimation of the calculation of the monitoring history of the node under consideration that makes the refinement of the expected time to get selfish by the node.

E. The Beta Probability Distribution for Detection of Selfish Nodes, Augmented with Estimation of Selfishness

The following are the values of parameters for Beta Probability Density Function, augmented with the consideration of selfishness of the nodes as per the mean rate of transmission of packets, to decide whether the node under consideration is selfish or malicious.

Lower Bound Value: 0 (These are the values between which the probabilities are considered)

Upper Bound Value: 1

α: Initially set to one (updated uniformly, considering selfishness)

β: Initially set to one (updated uniformly, considering cooperativeness)

The parameters α and β are updated regularly based on the estimate of the number of packets that are forwarded correctly by the neighboring nodes. These parameters estimate the value of cooperativeness and selfishness/maliciousness of the particular node under consideration. The proposed work is concerned with the effect of the fading factor on the values of these two parameters. The following table illustrates the parameter values considering Bayesian Filtering and selfishness information.

Table 2: Beta Probabilty Densitiy under Selfishness Consid-Eration

Round	α	β	Probability
0	1	1	0.5
1	0.89	1.11	0.575929
2	0.78	1.22	0.649978
3	0.67	1.33	0.720362
4	0.56	1.44	0.785489
5	0.45	1.55	0.844032
6	0.34	1.66	0.894995
7	0.23	1.77	0.93775
8	0.12	1.88	0.972052
9	0.01	1.99	0.998036

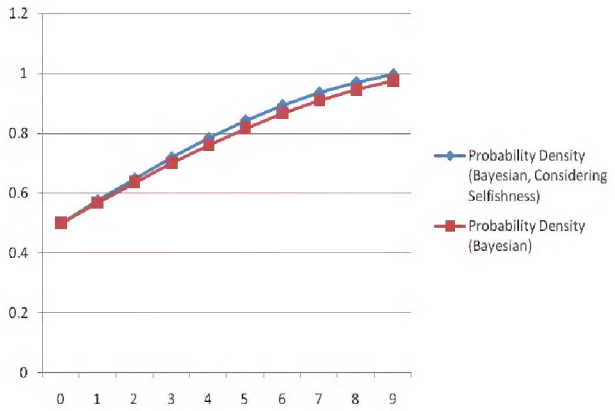

Figure 5: Probability Density Function as per Table 2

The high probability density function curve is in agreement with the theoretical setup that in addition to Bayesian statistics, the watchdog is also augmented with the additional information regarding the mean number of packets transferred by the nodes and the hardware implementation of the selfishness characteristics.

IV. CONCLUSIONS

The proposed method aimed at increasing the accuracy of the detection of selfish and/or malicious nodes behavior in P2P networks, as MANETs. One of the most significant problems of the standard watchdog is concerned with the influence of the noisy observation upon the accuracy. In this work, a new class of watchdogs is described that rely on Bayesian Statistics and mean time to get selfish. Bayesian filters are used in several scenarios due to their ability to reduce the influence of the noise on the measurements. In the standard watching, most of the false positives and false negatives are caused by the erroneous measurements of the packets that nodes should forward but actually they do not. The erroneous measurements are mostly caused by the unreliability of the wireless medium, but Bayesian Filtering can give a probabilistic estimate for the behavior of the node. A technique is devised to integrate Bayesian Filtering along with selfishness information, in standard watchdog implementation and simulations are conducted using Om NET++ to verify the approach. The integration of Bayesian filtering and Selfishness information, inside the watchdogs has decreased the

number of false positives detected while the percentage of the detection of the actual attacks has been kept quite high (or, even, slightly improved). As future work, it is intended to provide a concrete implementation of our Bayesian watchdog and to perform a deeper experimental phase on the real devices. Moreover, the approach to detect malicious nodes can be applied to other P2P networks (e.g., application overlay networks) by suitably modifying the concepts of what it is observed and what is the noisy (transmitted packets in MANETs, could be application messages in overlay networks, etc).

V. REFERENCES

1. Chlamtac, I., Conti, M., Liu, J.J.: "Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks" 1(1), 13–64 (2003), International Journal of Computer Applications (0985 – 8887) Volume 12– No.2, November 2010.
2. Buchegger, S., Boudec, J.Y.L.: "A robust reputation system for p2p and mobile ad-hoc networks (2004)" IEEE Transactions on Computers 47(10), October, 2008.
3. Ashish K. Maurya, Dinesh Singh ," Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocols in MANET", International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.
4. Truman, T.E., Pering, T., Doering, R., Brodersen, R.W. "The InfoPad Multimedia Terminal: A Portable Device for Wireless Information Access", IEEE Transactions on Computers 47(10), October, 2003.
5. Mohammad Reza Pasandideh, Marc St-Hilaire, "Automatic planning of 3G UMTS all-IP release 4 networks with realistic traffic", Computers & Operations Research, Volume 40, Issue 8, August 2013, Pages 1991-2003.
6. P. M. Mafra, J. S. Fraga, A.O. Santin, "Algorithms for a distributed IDS in MANETs", Journal of Computer and System Sciences, Volume 80, Issue 3, May 2013, Pages 554-570.
7. Khaled A. Ali, Hussein T. Mouftah, "Wireless personal area networks architecture and protocols for multimedia applications", Journal of Ad Hoc Networks, Volume 9, Issue 4, June 2011, Pages 675-686.
8. Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila, Pedro Peris-Lopez, "Evaluation of classification algorithms for intrusion detection in MANETs", Knowledge-Based Systems, Volume 36, December 2012, Pages 217-225.
9. Jun Li, Yifeng Zhou, Louise Lamont, F. Richard Yu, Camille-Alain Rabbath, "Swarm mobility and its impact on performance of routing protocols in MANETs", Computer Communications, Volume 35, Issue 6, 15 March 2012, Pages 709-719.
10. Fayez Khazalah, Ismail Ababneh, Zaki Malik, "Forwarding Group Maintenance of ODMRP in MANETs", Procedia Computer Science, Volume 19, 2013, Pages 289-296.
11. J. Manoranjini, A. Chandrasekar, D. Rajinigirinath, "Hybrid Detector for Detection of Black Holes in Manets", IERI Procedia, Volume 4, 2013, Pages 376-382.
12. Wang Bo, Huang Chuanhe, Li Layuan, Yang Wenzhong, "Trust-based minimum cost opportunistic routing for Ad hoc networks ", Journal of Systems and Software, Volume 84, Issue 12, December 2011, Pages 2107-212.

13. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in IEEE SPNA, 2002.

14. N. Bhalaji, A. Shanmugam, "Dynamic Trust Based Method to Mitigate Grey hole Attack in Mobile Adhoc Networks ", Procedia Engineering, Volume 30, 2012, Pages 881-88.

15. Christos Xenakis, Christoforos Panos, Ioannis Stavrakakis, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks", Computers & Security, Volume 30, Issue 1, January 2011, Pages 63-80.

16. Li LI, Yuan-an LIU, Bi-hua TANG, "SNMS: an intelligent transportation system network architecture based on WSN and P2P network", The Journal of China Universities of Posts and Telecommunications, Volume 14, Issue 1, March 2007, Pages 65-70.

17. Ali Moussaoui, Fouzi Semchedine, Abdallah Boukerram, "A link-state QoS routing protocol based on link stability for Mobile Ad hoc Networks", Journal of Network and Computer Applications, In Press, Corrected Proof, Available online 12 June 2011.

18. Tridib Mukherjee, Sandeep K.S. Gupta, Georgios Varsamopoulos, "Energy optimization for proactive unicast route maintenance in MANETs under end-to-end reliability requirements", Performance Evaluation, Volume 66, Issues 3–5, March 2009, Pages 141-15.

19. Lei Zhang, Jogesh K. Muppala, Samuel T. Chanson, "Integrated location management and location-aided routing system for mobile ad hoc networks", Journal of Parallel and Distributed Computing, Volume 66, Issue 3, March 2006, Pages 367-378.

20. S.S. Manvi, M.S. Kakkasageri, "Multicast routing in mobile ad hoc networks by using a multiagent system", Information Sciences, Volume 178, Issue 6, 15 March 2008, Pages 1611-162.

21. Qing Chen, Zubair Md. Fadlullah, Xiaodong Lin, Nei Kato, "A clique-based secure admission control scheme for mobile ad hoc networks (MANETs)", Journal of Network and Computer Applications, Volume 34, Issue 6, November 2011, Pages 1827-1835.

22. Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, Mehran S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains", Future Generation Computer Systems, Volume 25, Issue 8, September 2009, Pages 926-934

23. Guangjie Han, Jinfang Jiang, Lei Shu, Jianwei Niu, Han-Chieh Chao, "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of Computer and System Sciences, Volume 80, Issue 3, May 2014, Pages 602-617.

24. Honghuing Liu, Patrick P.C. Lee, John C.S. Lui, "On the credit evolution of credit-based incentive protocols in wireless mesh networks", Computer Networks, Volume 57, Issue 17, 9 December 2013, Pages 3327-3343.

25. Lamperter, B., Paul, K. Westhoff, "Charging support for MANET stub networks", Computer Communications 26, 1504-1514 (2013).